BAB II
LANDASAN TEORI

2.1. Jejaring Sosial

Jejaring sosial didefinisikan sebagai sekumpulan aktor sosial atau *node* yang terhubung dalam satu atau lebih relasi (Furht 2010). Aktor sosial atau *node* ini biasanya berupa individual, grup, atau organisasi. Aktor sosial atau *node* terhubung satu sama lain berdasarkan motif atau ketertarikan mereka (Grabner-Kräuter dan Mezgar 2015). Aspek penting dalam relasi jejaring sosial adalah tipe pertukaran informasi atau teknologi komunikasi didalamnya. Beberapa penelitian dibidang akademik menunjukan bahwa jejaring sosial beroperasi pada beberapa tingkatan, mulai dari tingkat keluarga hingga ke tingkat negara (Furht 2010). Jejaring sosial berperan penting dalam beberapa hal, seperti : menetukan cara penyelesaian suatu masalah, menjalankan suatu organisasi, serta menentukan sejauh mana seseorang dalam mencapai tujuannnya. Teknologi jejaring sosial mengambil berbagai bentuk termasuk majalah, forum internet, *weblog*, blog sosial, *microblogging*, *wiki, podcast*, foto atau gambar, video, peringkat dan *bookmark social*. Ciri-ciri jejaring sosial menurut Gamble (Gamble dan Kwal 2005) adalah sebagai berikut:

1. Pesan yang disampaikan tidak hanya untuk satu orang saja namun bisa ke berbagai banyak orang.
2. Pesan yang di sampaikan bebas, tanpa harus melalui suatu *Gatekeeper*.
3. Pesan yang disampaikan cenderung lebih cepat di banding media lainnya.
4. Penerima pesan yang menentukan waktu interaksi.

Jejaring sosial yang digunakan untuk penelitian ini adalah Facebook, Twitter, Instagram, Google Plus, Myspace, Pinterest, dan Reddit.

2.2. Format *File* Citra

Dalam prakteknya, data citra harus terlebih dahulu dimuat ke dalam memori dari sebuah *file* (Burger dan Burge 2016). *File* menyediakan mekanisme penting untuk pengarsipan, penyimpanan, dan pertukaran data citra. Untuk itu format citra adalah pilihan penting untuk sebuah aplikasi. Format *file* citra adalah bentuk standar untuk mengatur dan menyimpan gambar digital. *File* gambar terdiri dari data digital dalam suatu format yang dapat dirasterisasi untuk digunakan pada tampilan komputer atau printer. Format *file* citra dibagi dalam dua tipe, yaitu :

1. Format *Raster/Bitmap*

   Gambar berbasis *Raster* atau *Bitmap* adalah sebuah gambar yang terbentuk dari sekumpulan titik-titik (*pixel*). Setiap *pixel* atau *bit* pada gambar berisi informasi tentang warna yang akan ditampilkan. Semakin banyak jumlah *pixel* yang ada pada sebuah gambar, maka semakin halus dan realistik gambar tersebut. Format *file* yang biasanya digunakan adalah .BMP, .TIF, .JPG, .GIF, dan .PNG.

2. Format *Vector*

   Merupakan gambar digital yang disusun dari kumpulan garis-garis dan kurva-kurva yang disusun secara matematika (komputer mencatat posisi titik ujung dan pangkalnya sesuai dengan posisi koordinatnya masing-masing). Ukuran *file* relatif kecil dan jika diubah ukurannya, kualitasnya tidak berubah. Format *file* yang biasanya digunakan adalah .EPS, .AI, dan .SVG.

2.2.1. *Joint Photographic Experts Group* (JPEG)

JPEG merupakan metode kompresi *lossy* (Burger dan Burge 2016). Citra dari kompresi ini disimpan dalam format *file* JFIF (*JPEG File Interchange Format*) dengan ekstensi .JPG atau .JPEG. Format *file* Exif adalah format terbaru untuk kompresi JPEG. Exif biasanya digunakan pada hasil gambar dari kamera digital. JPEG mendukung tipe citra *greyscale* dan citra *truecolor*. Format ini paling banyak digunakan dan sudah menjadi format umum untuk fotografi.

Struktur *metadata* JPEG terdiri dari urutan segmen yang biasanya dimulai dengan *marker*. Setiap *marker* dimulai dengan hexa FF dan diikuti dengan hexa yang mengindikasikan *marker* tersebut. Segment-segmen yang ada pada JPEG dapat dilihat pada Tabel 2.1.

Tabel 2.1 Struktur *File* atau Segmen pada JPEG

Segmen	Hexa	Panjang	Nama	Deskripsi
SOI	0xFF, 0xD8	Tidak ada	Start Of Image	*Marker* awal JPEG
SOF0	0xFF, 0xC0	Bervariasi	Start Of Frame (baseline DCT)	Indikasi untuk *encoding* yang digunakan. *Encoding* yang digunakan adalah *baseline DCT*
SOF2	0xFF, 0xC2	Bervariasi	Start Of Frame (progressive DCT)	Indikasi untuk *encoding* yang digunakan. *Encoding* yang digunakan adalah *progressive DCT*
DHT	0xFF, 0xC4	Bervariasi	Define Huffman Table(s)	*Marker* untuk *Huffman table*.
DQT	0xFF, 0xDB	Bervariasi	Define Quantization Table(s)	*Marker* untuk *quantization table*.
DRI	0xFF, 0xDD	4 bytes	Define Restart Interval	Menentukan interval antara *marker* RSTn, dalam *Minimum Coded Units* (MCU). *Marker* ini diikuti oleh dua *byte* yang menunjukkan ukuran tetap sehingga dapat diperlakukan seperti segmen ukuran variabel lainnya.
SOS	0xFF, 0xDA	Bervariasi	Start Of Scan	Memulai pemindaian gambar dari atas ke bawah. Pada JPEG *baseline DCT*, umumnya ada satu pemindaian. Pada JPEG *progressive DCT* biasanya mengandung beberapa pemindaian. *Marker* ini menentukan data mana yang akan diisi, dan diikuti oleh data *entropy-code*.
RST*n*	0xFF, 0xD*n* (*n*=0..7)	Tidak ada	Restart	Memasukan setiap *r macroblock*, dimana *r* adalah set *restart interval* dari DRI *marker*. Tidak akan digunakan jika tidak ada DRI *marker* pada gambar.
APP*n*	0xFF, 0xE*n*	Bervariasi	Application-specific	Segmen yang menyimpan informasi format.
COM	0xFF, 0xFE	Bervariasi	Comment	Berisi teks komentar
EOI	0xFF, 0xD9	Tidak ada	End Of Image	*Marker* akhir JPEG

Untuk setiap *marker*, terdapat identifikasi *marker* dan panjang *marker*. Data yang diikuti setelah dua data tersebut berbeda-beda untuk setiap *marker*. Berikut contoh data *marker* SOF0 pada Tabel 2.2. *Marker* ini digunakan untuk menyimpan informasi *encoding baseline* DCT yang digunakan pada gambar.

Tabel 2.2 Struktur pada *marker* SOF0

Field	Panjang	Deskripsi
Marker Identifier	2 bytes	Penanda *marker* SOF0
Length	2 bytes	Nilai panjang segment = 8 + 3 nilai *component*
Data precision	1 bytes	Bit presisi untuk komponen sample pada gambar. Dihitung dalam *bits/sample*, biasanya 8 (12 dan 16 tidak didukung kebanyakan *software*).
Image height	2 bytes	Panjang gambar. Harus > 0
Image Width	2 bytes	Lebar gambar. Harus > 0
Number of components	1 bytes	Biasanya 1 = *grey scale*, 3 = YcbCr atau YIQ, 4 = CMYK
Untuk setiap component	3 bytes	Terdapat *component* Id(1byte)(1 = Y, 2 = Cb, 3 = Cr, 4 = I, 5 = Q), *sampling factors* (1byte) (bit 0-3 vertical., 4-7 horizontal.), dan *quantization table number* (1 byte).

Marker APPn merupakan segmen yang digunakan untuk menyimpan informasi aplikasi format gambar. APP0 digunakan untuk menyimpan informasi standar untuk sebuah gambar. Keterangan data pada segmen ini dapat dilihat pada Tabel 2.3.

Tabel 2.3 Struktur pada segmen APP0

Field	Panjang	Deskripsi
Marker Identifier	2 bytes	Penanda *marker* APP0
Length	2 bytes	Panjang *marker*. Harus >= 16
File Identifier Mark	5 bytes	Mengidentifikasikan format (JFIF)
Major revision number	1 bytes	Harus bernilai 1
Minor revision number	1 bytes	Harus bernilai antara 0 dan 2
Units for x/y densities	1 bytes	0 = tidak ada unit, x/y-density mengindikasikan *aspect ratio*. 1 = x/y-density untuk *dots/inch*, 2 = x/y-density untuk *dots/cm*
X-density	2 bytes	Harus <> 0
Y-density	2 bytes	Harus <> 0
Thumbnail width	1 bytes	---
Thumbnail height	1 bytes	---

APP1_Exif adalah segmen untuk menyimpan data atau informasi format Exif. Pada format ini informasi dapat berupa waktu atau tanggal gambar ini diambil, konfigurasi kamera yang digunakan dalam pengambilan gambar, keterangan hak cipta gambar, dan lain-lain. Informasi ini disimpan pada *padding byte*. Keterangan data pada segmen ini dapat dilihat pada Tabel 2.4.

Tabel 2.4 Struktur segmen APP1_Exif

Field	Panjang	Deskripsi
Marker Identifier	2 bytes	Penanda *marker* APP1_Exif
Length	2 bytes	Panjang *marker*
Padding byte	Bervariasi	Panjang *byte* yang digunakan untuk menyimpan informasi Exif

APP2_ICC merupakan segmen untuk menyimpan informasi profil warna pada gambar. Jika gambar memiliki segmen ini, gambar tersebut memiliki informasi ruang warna yang berbeda dari gambar standar. Data pada segmen ini dapat dilihat pada Tabel 2.5. Untuk segmen APP penomoran lainnya, data atau informasi yang disimpan merupakan informasi mengenai aplikasi pemrosesan gambar tersebut.

Tabel 2.5 Struktur segmen APP2_ICC

Field	Panjang	Deskripsi
Marker Identifier	2 bytes	Penanda *marker* APP2_ICC
Length	2 bytes	Panjang *marker*.
File Identifier Mark	12 bytes	Mengidentifikasikan ICC_Profile
Padding byte	Bervariasi	Panjang *byte* yang digunakan untuk menyimpan informasi ruang warna

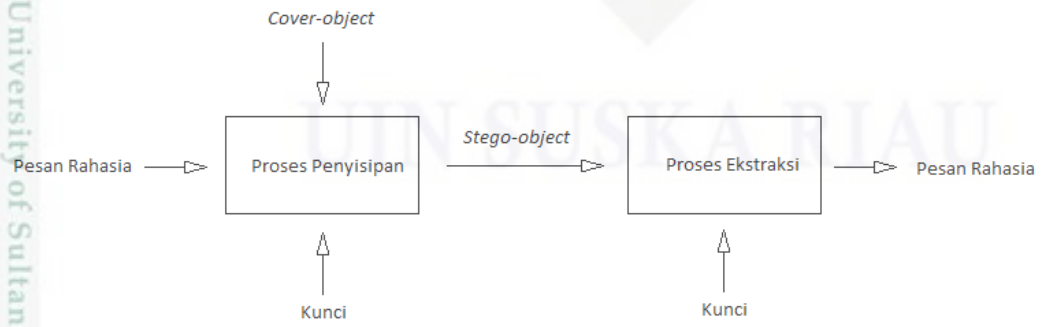
2.2.2. JPEG-2000

Format JPEG-2000 menggunakan kompresi *lossless* dan *lossy* (Burger dan Burge 2016). Format ini menggunakan metode kompresi yang berbeda dari JPEG, dimana pada kompresi JPEG-2000 terjadi peningkatan kualitas dan rasio kompresi. Kelemahan dari kompresi format ini adalah membutuhkan komputasi lebih besar untuk diproses.

2.3. Steganografi

Steganografi adalah sebuah seni menyembunyikan pesan sedemikian rupa sehingga keberadaan pesan tersebut tidak dapat dideteksi oleh orang lain (Munir 2004). Sebaliknya, kriptografi menyamarkan arti dari suatu pesan, tapi tidak menyembunyikan bahwa ada suatu pesan. Steganografi membutuhkan dua properti, *hidden message* sebagai pesan rahasia yang akan disembunyikan dan *cover-object* sebagai wadah penampung untuk menyembunyikan pesan rahasianya. Proses menyembunyikan pesan ke dalam *cover-object* akan menghasilkan *stego-object*. *Stego-object* adalah data yang telah disisipi pesan rahasia di dalamnya. Dalam media digital, wadah penampung dan data rahasia yang akan disembunyikan dapat berupa citra, suara, text, dan video. Proses steganografi dapat dilihat pada Gambar 2.1. Steganografi yang bagus harus memiliki kriteria sebagai berikut:

a. *Fidelity*. Kualitas *stego-object* tetap terjaga dan tidak jauh berubah dari *cover-object*. *Stego-object* tidak dapat di persepsi oleh orang lain.
b. *Robustness*. Data atau pesan tersembunyi di dalam *stego-object* tahan dari manipulasi. Jika terjadi operasi pengolahan pada *stego-object*, pesan atau data di dalamnya tidak rusak dan tetap utuh.
c. *Recovery*. Data atau pesan yang tersembunyi di dalam *stego-object* harus dapat diungkapkan kembali.



Gambar 2.1 Proses Steganografi

Tujuan dari steganografi adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi. Dalam

prakteknya, kebanyakan pesan disembunyikan dengan membuat perubahan kecil terhadap *stego-object* yang isinya tidak akan menarik perhatian dari penyerang potensial, sebagai contoh sebuah gambar yang terlihat tidak berbahaya. Perubahan ini bergantung pada kunci dan pesan yang disembunyikan. Orang yang menerima gambar kemudian dapat menyimpulkan informasi tersembunyi dengan cara memasukan kembali kunci yang benar ke dalam algoritma yang digunakan.

2.3.1. Teknik Dasar dalam Steganografi

Teknik dasar steganografi dibagi berdasarkan penerapan modifikasi *cover-object* saat melakukan proses penanaman pesan rahasia (Katzenbeisser dan Petitcolas 2000).

2.3.1.1. Teknik *Substitusi*

Saat melakukan proses penanaman pesan rahasia, bagian yang redundan dari *cover-object* diganti dengan *bit-bit* pesan rahasianya (Katzenbeisser dan Petitcolas 2000). Contoh metode yang menggunakan teknik ini adalah : *Least Significant Bit* (LSB), Permutasi *Pseudorandom, Image Downgrading* dan *Covert Channel, Cover-Regions* dan *Parity Bits, Palette-Based Image,* serta *Quantization* dan *Dithering.*

2.3.1.2. Teknik *Transform Domain*

Teknik *Transform Domain* menyembunyikan pesan di dalam daerah yang signifikan pada *cover-object*, yang membuat teknik ini lebih tahan terhadap manipulasi *stego-object* (Katzenbeisser dan Petitcolas 2000). Metode yang menggunakan teknik ini adalah : Steganografi *DCT Domain, Phase Coding, Echo Hiding,* serta *Information Hiding* dan *Data Compression*.

2.3.1.3. Teknik *Spread Spectrum*

Teknik ini menyisipkan data atau pesan rahasia dengan mengadopsi ide komunikasi *spread spectrum* (Katzenbeisser dan Petitcolas 2000). Teknik *spread spectrum* adalah sarana transmisi di mana sinyal menempati sebuah *bandwidth* yang melebihi syarat minimum untuk mengirimkan informasi.

2.3.1.4. Teknik *Statical*

Teknik ini menyisipkan pesan dengan mengubah beberapa properti statistik dari *cover-object* dan menggunakan metode uji hipotesis pada proses ekstraksi pesan (Katzenbeisser dan Petitcolas 2000).

2.3.1.5. Teknik *Distortion*

Teknik ini menyimpan pesan rahasia dengan distorsi sinyal dan mengukur deviasinya dari *cover-object* pada proses ekstraksi pesan (Katzenbeisser dan Petitcolas 2000).

2.3.1.6. Teknik *Cover Generation*

Teknik ini tidak menyisipkan pesan pada *cover-object* yang dipilih secara acak dan tidak menggunakan algoritma untuk menyisipkan pesan ke dalam *cover-object.* Teknik ini dimaksudkan hanya untuk melakukan komunikasi rahasia. Penyisipan pesan rahasia menggunakan beberapa fitur yang ada pada *cover-object*nya sebagai ruang untuk menyisipkan pesan, contohnya seperti metadata pada *cover-object* (Katzenbeisser dan Petitcolas 2000).

2.4. Steganografi pada Jejaring Sosial

Jejaring sosial yang ada saat ini telah memungkinkan penggunanya untuk berbagi konten multimedia seperti foto dan video. Hal ini memungkinkan seseorang untuk menyisipkan pesan rahasia ke dalam konten multimedia tersebut. Penelitian yang dilakukan oleh Viejo (Viejo et al. 2013) membuktikan bahwa steganografi dapat dilakukan pada jejaring sosial. Penelitian ini bertujuan untuk menyembunyikan data profil pengguna jejaring sosial ke dalam sebuah gambar yang diunggah pada jejaring sosial tersebut. Data profil asli pengguna hanya dapat diakses oleh pengguna tertentu, sedangkan data profil yang ada pada jejaring sosial hanyalah data palsu. Jejaring sosial yang digunakan pada penelitian Viejo adalah facebook. Facebook melakukan pengolahan pada gambar yang diunggah, sehingga Viejo membuat algoritma khusus agar pesan yang disisipi dapat diungkap kembali.

Castiglione (Castiglione et al. 2011) pada penelitiannya yang berjudul *Steganography and Secure Communication on Online Social Networks and Online Photo Sharing*, juga membuktikan steganografi dapat diterapkan pada jejaring sosial. Penelitian yang dilakukan Castiglione bertujuan untuk menggunakan steganografi sebagai saluran komunikasi rahasia. Teknik yang digunakan pada penelitian ini adalah dengan memanfaatkan *metadata* sebuah citra sebagai tempat penyimpanan pesan rahasianya. Pesan rahasia disisipkan ke dalam salah satu attribut *metadata* seperti nama *file* atau kolom komentar. Castiglione memanfaatkan fitur *tag* yang ada pada jejaring sosial sebagai pemberitahuan kepada penerima dalam melakukan komunikasi rahasia.

2.5. *Stegosploit*

Sebuah exploitasi yang diberi nama *Stegospoit* ditemukan oleh Saumil Shah pada tahun 2015 (Shah 2015). *Stegospoit* merupakan sebuah teknik yang memungkinkan pelaku menyembunyikan sebuah *script* dalam *metadata* suatu gambar yang dapat mengekploitasi korbannya hanya dengan membuka gambar tersebut. Exploit ini menggunakan steganografi untuk menyisipkan *script* ke dalam gambar. Untuk mengeksekusi *script* dalam gambar, dibutuhkan sebuah *decoder*. *Decoder* ini hanya berisi *script* untuk memanggil *script* lain, jadi dapat dikatakan aman dari pelacakan keamanan sistem, karena tidak mengandung *script* berbahaya. *Payload* adalah *script* yang disisipi ke dalam gambar. *Script* ini aman dari pelacakan keamanan sistem, sekalipun *payload* berisi *script* yang membahayakan. Hal ini dikarenakan *payload* hanya dapat dijalankan oleh *decoder*.

Cara kerja *stegosploit* adalah pada saat gambar yang mengandung *payload* didalamnya dibuka pada *web browser*, pada saat itu *decoder* melakukan *scanning* ke gambar yang dibuka. *Scanning* dilakukan pada *metadata* gambar. Seteleah *script* ditemukan pada gambar, maka *decoder* mengeksekusi *script payload* yang ada dalam gambar. Tujuan utama *script* disembunyikan pada *metadata* gambar adalah untuk menghindari *script* dari pemeriksaan keamanan pada *server*. *Decoder code* untuk eksploit ini disimpan pada *web server* dimana

gambar itu disimpan, atau dapat juga disimpan pada *web extension/add-on web browser* untuk menjalankannya pada situs milik orang lain.

2.6. Steganalisis

Steganalisis merupakan ilmu atau seni untuk mendeteksi keberadaan pesan atau informasi rahasia yang tersembunyi dalam suatu objek (Cox et al. 2008). Proses steganalisis ini membutuhkan beberapa bentuk aksi, yaitu menemukan, mengungkapkan, mengubah, dan melumpuhkan pesan rahasia (Katzenbeisser dan Petitcolas 2000). Terdapat dua tipe pendeteksian, yaitu *Targeted Steganalysis* dan *Blind Steganalysis* (Cox et al. 2008). *Targeted Steganalysis* merupakan pendeteksian yang dimaksudkan untuk algoritma steganografi yang spesifik dan terkadang dibatasi hanya pada format media tertentu saja. Teknik ini mempelajari dan menganalisis algoritma penyisipan, lalu menemukan statistik yang berubah setelah penyisipan. Hasil steganalisis sangat akurat, tetapi tidak fleksibel karena tidak dapat diperluas untuk algoritma steganografi yang lain atau format media yang berbeda.

Blind Steganalysis adalah pendeteksian yang dimaksudkan untuk algoritma steganografi dalam cakupan yang luas. Teknik ini bekerja pada sembarang algoritma steganografi dan sembarang format media. Teknik ini mempelajari perbedaan antara statistik *cover-object* dan *stego-object* dan membedakannya. Proses pembelajaran (*learning*) dilakukan dengan melatih (*training*) mesin pada sekumpulan *database* media. Model *machine learning* yang digunakan misalnya jaringan syaraf tiruan. Hasil steganalisis kurang akurat dibandingkan dengan teknik *targeted steganalysis*, tetapi kelebihannya adalah dapat diperluas untuk algoritma yang lain. Pendeteksian algoritma steganografi juga dapat diterapkan dengan melakukan exploitasi dari kelemahan algoritma steganografi tersebut.

Metode steganalisis dibagi dalam dua bentuk, yaitu : *Visual Attack* dan *Statistical Attack.*

1. Serangan berbasis visual (*visual attack*)

Metode ini dikhususkan untuk *stego-object* berupa citra. Metode ini bersifat subjektif, karena melakukan pengamatan secara kasat mata dengan melihat artefak yang mencurigakan di dalam *stego-image*, lalu membandingkannya dengan citra asli (*cover image*). Biasanya metode ini digunakan pada awal riset steganalisis. Contoh metode steganalisis serangan berbasis visual adalah LSB *plane attack* dan *Filtered visual attack* (*Enhanced* LSB).

2. Serangan berbasis statistik (*statistical attack*)

   Metode ini menggunakan analisis matematik pada citra untuk menemukan perbedaan antara *cover-image* dengan *stego-image*. Didasarkan pada fakta bahwa penyembunyian pesan kedalam media menimbulkan artefak yang dapat dideteksi secara statistik sehingga dapat mengungkap penyembunyian pesan atau pesan yang disembunyikan itu sendiri. Contoh metode steganalisis serangan statistik adalah *Histogram analysis*, *Regular-singular*(RS) *analysis*, *Chi-square analysis*, dan *Sample pair* (SP) *analysis*.

2.7. Solusi Untuk Ancaman Steganografi pada Jejaring Sosial

Steganografi dapat menjadi sebuah ancaman jika digunakan oleh orang-orang yang salah. Pada tahun 2008, data finansial Departemen Kehakiman Amerika berhasil dicuri (Wendzel dan Mazurczyk 2014). Hal ini ditemukan dari sebuah gambar yang disisipi data tersebut. Pada tahun 2010, informasi rahasia Amerika bocor ke tangan mata-mata Rusia. Informasi tersebut dikirim ke Rusia menggunakan steganografi agar tidak diketahui oleh Amerika. Namun akhirnya mata-mata tersebut tertangkap di New York. Selain digunakan untuk tujuan keamanan, steganografi juga dapat menjadi ancaman serius.

Berdasarkan penelitian mengenai steganografi pada jejaring sosial (Castiglione et al. 2011; Viejo et al. 2013), serta masalah serius pada steganografi (Wendzel dan Mazurczyk 2014), Rathore (Rathore et al. 2017) menjadikan steganografi sebagai salah satu ancaman pada jejaring sosial. Dengan adanya fitur berbagi konten multimedia pada jejaring sosial, pelaku kejahatan dapat

memanfaatkan fitur ini untuk kejahatannya. Mereka dapat mengunggah *file* yang telah disisipi informasi berbahaya ke jejaring sosial. Pengguna lain bisa saja mengunduh *file* berbahaya ini tanpa mengetahui *file* tersebut telah disisipi informasi berbahaya. Hal ini tentunya bisa merusak reputasi jejaring sosial dan membahayakan pengguna yang mengunduh *file* berbahaya tersebut. Untuk menghadapi masalah ini, Rathore memberikan beberapa solusi, yaitu : steganalisis, *spam detection, web security software*, dan laporan pengguna (*report user*).

2.7.1. Steganalisis pada Jejaring Sosial

Salah satu contoh yang menerapkan steganalisis pada jejaring sosial terdapat pada penelitian Natarajan (Natarajan, Sheen, dan Anitha 2015). Penelitian yang dilakukan oleh Natarajan merancang sebuah pendekatan identifikasi *multilevel* yang mana melakukan identifikasi untuk setiap profil yang mencurigakan pada jejaring sosial. Pendekatan ini melakukan analisa pada sejumlah besar data citra yang ada pada tiap profil jejaring sosial. Dengan begitu banyaknya data yang akan dianalisa, penelitian ini menghadapi masalah dalam melakukan analisa secara *real-time*. Untuk skala jejaring sosial yang lebih besar, Fengyong Li mengajukan mekanisme yang menggunakan fitur *high-order joint* dan *clustering ensemble* (Fengyong Li et al. 2016). Fitur *high-order joint* melatih semua hirarki *sub-clustering*, dan *output* tiap *sub-clustering* akan disatukan menjadi *clustering ensemble* menggunakan *voting* mayoritas. *Cluster ensemble* inilah yang akan digunakan untuk menyaring citra mencurigakan.

Sebuah metode diajukan oleh Venkatachalam pada penelitiannya untuk mendeteksi akun yang menggunakan steganografi (Venkatachalam dan Anitha 2017). Teknik ini menggunakan kombinasi fitur grafik sosial pengguna, akun pengguna, dan konten multimedia citra pengguna untuk mengidentifikasi tingkah laku mencurigakan dari sebuah akun. Teknik ini terbukti efektivitasnya pada jejaring sosial google plus, twitter, facebook, dan flickr.

2.7.2. *Spam Detection*

Penerapan *spam detection* pada jejaring sosial terdapat pada penelitian Hai Wang dkk (Wang 2010). Penelitian ini mendeteksi akun spam pada jejaring

sosial twitter berdasarkan grafik sosial dan konten. Penelitian ini mengumpulkan *dataset* asli dari informasi yang tersedia secara publik dan menggunakannya sebagai *input* untuk membedakan kiriman *spam* dengan kiriman yang sebenarnya. Penelitian yang dilakukan Lee (Lee, Caverlee, dan Webb 2010) menggunakan pendekatan berbasis *social honeypod* untuk mengidentifikasi *spam* pada myspace dan twitter. Pendekatan ini mengumpulkan *dataset* asli dari komunitas jejaring sosial menggunakan *social honeypots.* Ahmed memperkenalkan skema statistik umum untuk mengidentifikasi akun *spam* pada facebook dan twitter (Ahmed dan Abulaish 2013). Pada penelitiannya, Ahmed mengajukan empat belas statistik umum untuk memvalidasi efektivitas skemanya.

2.7.3. *Web Security Service*

Salah satu cara yang disarankan oleh Rathore (Rathore et al. 2017) untuk menghadapi ancaman steganografi adalah dengan memasang perangkat lunak pihak ketiga atau *plugin* pendukung yang tersedia di internet. Contoh *web security service* adalah *anti-virus, add-on browser*, aplikasi yang disediakan penyedia jejaring sosial, serta program proteksi lainnya.

2.7.4. *Report User*

Solusi ini dilakukan oleh pengguna dan dieksekusi oleh layanan jejaring sosial. Solusi ini membutuhkan pengguna jejaring sosial untuk mengetahui sifat-sifat *file* yang mencurigakan. Jika pengguna menemukan *file* mencurigakan, tindakan yang dilakukan adalah melaporkan *file* tersebut ke pihak jejaring sosial untuk diproses. Selanjutnya hanya perlu menunggu tanggapan dari jejaring sosial tersebut.

2.8. Penelitian Terkait

Berikut adalah beberapa penelitian terkait tentang steganografi dan sistem keamanan pada jejaring sosial :

1. Penelitian tentang keamanan jejaring sosial yang berjudul "*Social network security: Issues, challenges, threats, and solutions*" oleh Rathore Shailendra, Sharma Pradip Kumar, Loia Vincenzo, Jeong

Young Sik, dan Park Jong Hyuk tahun 2017. Layanan jejaring sosial menjadi celah resiko penyerangan keamanan *cyber*. Penelitian ini mempelajari mengenai beberapa masalah keamanan dan privasi pengguna jejaring sosial yang meningkat sejak munculnya beberapa fitur seperti berbagi gambar, melakukan *tagging*, *blogging*, dan lain-lain. Penelitian ini menghasilkan sebuah teknik yang mudah digunakan untuk merespon ancaman-ancaman bagi pengguna jejaring sosial sebagai perlindungan.

2. Penelitian tentang keamanan jejaring sosial yang berjudul "*An Analysis of Security in Social Networks* " oleh Luo Weimin, Liu Jingbo, Liu Jing, dan Fan Chengyu tahun 2009. Penelitian ini mempelajari ancaman pada jejaring sosial dan menganalisa apa yang diinginkan oleh penyerang serta metode yang mereka gunakan. Penelitian ini mendiskusikan bagaimana melawan serangan-serangan yang ada pada jejaring sosial. Hasil dari penelitian ini adalah sebuah usulan *framework* keamanan untuk jejaring sosial.
3. Penelitian tentang steganografi pada jejaring sosial yang berjudul "*Preserving the User's Privacy in Social Networking Sites*" oleh Alexandre Viejo, Jordi Castellà-Roca, dan Guillem Rufián tahun 2013. Penelitian ini mengusulkan sebuah sistem penjaga privasi profil pengguna jejaring sosial untuk mengatur siapa saja yang dapat mengaksesnya. Penelitian ini menggunakan steganografi untuk menyembunyikan data pribadi asli pengguna dalam gambar profil jejaring sosial. Penelitian ini menghasilkan sebuah kesimpulan bahwa sistem ini dapat berjalan pada jejaring sosial facebook dan data asli pengguna tidak dapat dilihat oleh entitas yang tidak diberikan hak.
4. Penelitian tentang steganografi pada jejaring sosial yang berjudul "*Steganalysis Over Large-Scale Social Networks With High-Order Joint Features and Clustering Ensembles*" oleh Li Fengyong, Wu

Kui, Lei Jingsheng, Wen Mi, Bi Zhongqin, dan Gu Chunhua tahun 2016. Untuk mendeteksi *steganographer* yang ada pada jejaring sosial skala besar, penelitian ini mengusulkan sebuah metode yang menggunakan *high-order joint feature* dan *clustering ensemble*. Hasil penelitian ini menunjukan bahwa metode yang diajukan efektif dan efisien dalam mengindentifikasi *steganographer* dalam jejaring sosial skala besar.

5. Penelitian tentang keamanan jejaring sosial yang berjudul "*Multilevel Analysis to Detect Covert Social Botnet in Multimedia Social Networks*" oleh V. Natarajan, Shina Sheen dan R. Anitha tahun 2014. Penelitian ini mengajukan sebuah metode yang efektif untuk mendeteksi *host stegobot* pada jejaring sosial. Untuk meningkatkan kemampuan deteksi, model klasifikasi dirancang menggunakan analisa *profile level* dan *content level*. Penelitian ini mendapatkan hasil akurasi pendeteksian sebesar 97%.
6. Penelitian tentang keamanan jejaring sosial yang berjudul "*A multi-feature approach to detect Stegobot: a covert multimedia social network botnet*" oleh Natarajan Venkatachalam dan R. Anitha tahun 2016. Fokus utama penelitian ini adalah untuk mendeteksi profil pengguna jejaring sosial apakah profil tersebut sebuah *bot* atau bukan. Sebuah fitur berdasarkan *social graph* akun pengguna jejaring sosial dapat mengidentifikasi komunikasi *stegobot*. Hasil penelitian ini juga dapat berguna untuk analisa forensik jaringan.